# HHS.gov

U.S. Department of Health & Human Services

**Health Information Privacy**

## Your Rights Under HIPAA

**This guidance remains in effect only to the extent that it is consistent with the court's order in Ciox Health, LLC v. Azar, No. 18-cv-0040 (D.D.C. January 23, 2020), which may be found at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51. More information about the order is available at https://www.hhs.gov/hipaa/court-order-right-of-access/index.html. Any provision within this guidance that has been vacated by the Ciox Health decision is rescinded.**

Most of us believe that our medical and other health information is private and should be protected, and we want to know who has this information. The Privacy Rule, a Federal law, gives you rights over your health information and sets rules and limits on who can look at and receive your health information. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Security Rule is a Federal law that requires security for health information in electronic form.

### HIPAA Right of Access Videos

OCR has teamed up with the HHS Office of the National Coordinator for Health IT to create ***Your Health Information, Your Rights!***, a series of three short, educational videos (in English and option for Spanish captions) to help you understand your right under HIPAA to access and receive a copy of your health information.

- Individual's Right under HIPAA to Access their Health Information

- HIPAA Access Associated Fees and Timing
- HIPAA Access and Third Parties

## HIPAA Right of Access Infographic

OCR has teamed up with the HHS Office of the National Coordinator for Health IT to create this one-page fact sheet, with illustrations, that provides an overall summary of your rights under HIPAA:

- Your Health Information, Your Rights! - PDF

## HIPAA General Fact Sheets

- Your Health Information Privacy Rights - PDF
- Privacy, Security, and Electronic Health Records - PDF
- Sharing Health Information with Family Members and Friends - PDF

## Who Must Follow These Laws

We call the entities that must follow the HIPAA regulations "covered entities."

Covered entities include:

- **Health Plans**, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- **Most Health Care Providers**—those that conduct certain business electronically, such as electronically billing your health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- **Health Care Clearinghouses**—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

In addition, business associates of covered entities must follow parts of the HIPAA regulations.

Often, contractors, subcontractors, and other outside persons and companies that are not employees of a covered entity will need to have access to your health information when providing services to the covered entity. We call these entities “business associates.” Examples of business associates include:

- Companies that help your doctors get paid for providing health care, including billing companies and companies that process your health care claims

- Companies that help administer health plans
- People like outside lawyers, accountants, and IT specialists
- Companies that store or destroy medical records

Covered entities must have contracts in place with their business associates, ensuring that they use and disclose your health information properly and safeguard it appropriately. Business associates must also have similar contracts with subcontractors. Business associates (including subcontractors) must follow the use and disclosure provisions of their contracts and the Privacy Rule, and the safeguard requirements of the Security Rule.

## Who Is Not Required to Follow These Laws

Many organizations that have health information about you do not have to follow these laws**.**

**Examples of organizations that do not have to follow** the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

## What Information Is Protected

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer’s computer system
- Billing information about you at your clinic

- Most other health information about you held by those who must follow these laws

## How This Information Is Protected

- Covered entities must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.
- Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- Covered entities must have procedures in place to limit who can view and access your health information as well as implement training programs for employees about how to protect your health information.
- Business associates also must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.

## What Rights Does the Privacy Rule Give Me over My Health Information?

Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can
  - File a complaint with your provider or health insurer
  - File a complaint with HHS

You should get to know these important rights, which help you protect your health information.

You can ask your provider or health insurer questions about your rights.

Learn more about your health information privacy rights - PDF.

## Who Can Look at and Receive Your Health Information

The Privacy Rule sets rules and limits on who can look at and receive your health information

To make sure that your health information is protected in a way that does not interfere with your health care, your information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes or sell your information

**Sign Up for the OCR Privacy Listserv**
Keep up-to-date as OCR releases updated health information privacy FAQs, guidance, and technical assistance materials.

Content created by Office for Civil Rights (OCR)

Content last reviewed on November 2, 2020